PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 11 August 2000 (11.08.00)	
International application No. PCT/GB99/04219	**Applicant's or agent's file reference** 23680
International filing date (day/month/year) 20 December 1999 (20.12.99)	**Priority date** (day/month/year) 18 December 1998 (18.12.98)
Applicant JARMAN, David, Michael	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

18 July 2000 (18.07.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Pascal Piriou
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

14

PATENT COOPERATION TREATY

REC'D 22 MAR 2001
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
23680		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB99/04219	20/12/1999	18/12/1998
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant JARMAN, David, Michael		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
18/07/2000	20.03.2001
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Van de Maele, L Telephone No. +49 89 2399 8805

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB99/04219

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

1,3-11	as originally filed			
2	as received on	04/01/2001	with letter of	29/12/2000

Claims, No.:

1-19	as received on	04/01/2001	with letter of	29/12/2000

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   ☐ the language of publication of the international application (under Rule 48.3(b)).
   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:
   ☐ the claims, Nos.:
   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2-12,14-19
	No:	Claims	1,13
Inventive step (IS)	Yes:	Claims	8-12,16-19
	No:	Claims	1-7,13-15
Industrial applicability (IA)	Yes:	Claims	1-19
	No:	Claims	

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Cited documents:

D1: WO 98 08344 A
D2: FR 2 681 165 A

Re. sections V and VIII

1.a Apparatus **claim 1**

The subject-matter of **claim 1** does not appear to involve an inventive step having regard to the prior art disclosed D1.

D1 namely already describes, in correspondence with the preamble of **claim 1**, an apparatus for reception, storage and display of data in electronic format (D1, abstract and fig. 1, "14"). This apparatus also comprises data storage means, data display means and data transmission/reception means (D1, page 7, paragraph 3). Received data is decrypted and stored in the data storage means (D1, page 7, paragraph 3). It is not known from D1 to perform decryption in the reception means, however, D1 (page 7, third paragraph) teaches that this can be done by any combination of soft- and hardware and therefore selecting the reception means for this purpose is just one of the alternatives among which a skilled person would select. The apparatus of D1 also comprises storage means for storing an encryption key (D1, page 10, first paragraph).

According to the characterizing part of **claim 1**, the encryption key is only used to address the ROM to find the decryption key for the received data. Moreover, there are no features in **claim 1** which define a use of that key for encrypting. Therefore, this key is merely an index or pointer to the decryption key stored ROM of the apparatus. Document D2, which also describes an apparatus for receiving encrypted data, already teaches the use of an index into ROM (D2, page 4, lines 2 to 9) to retrieve the decryption key and to use the latter for decrypting the received data.

The apparatus defined in **claim 1** can not only receive encrypted data, decrypt it and store it in memory, it can also process the data in the reverse manner. It is

however explicitly indicated in D1 that this can also be done with the apparatus described therein (D1, page 6, first paragraph).

Therefore, all features of the claimed subject-matter of **claim 1** are known from D1 and D2. Both documents relate to the same problem of exchange of electronic information in encrypted form and thus the skilled person would consider combining the features known from these documents. Therefore, **claim 1** does not meet the requirements of *Article 33(3) PCT*.

1.b Dependent **claims 2 to 7**

The features of the dependent **claims 2, 5 and 7** are also already known from D1 (D1, pages 3. 7 and 10).

The features of **claims 3, 4** merely represent a choice of the key and memory size which does not appear to be relevant

Claim 6 merely defines the use of a well known type of communication link.

Therefore, none of the dependent claims appears to add an inventive step to the subject-matter of **claim 1** and thus also these claims do not meet the requirements of *Article 33(3) PCT*.

2.a Independent method **claim 13**

Claim 13 appears to merely define a method for transmitting encrypted data between two devices. Merely as an example, prior art document D1 already describes (D1, page 7, second paragraph) such a method for transmitting encrypted data from an apparatus (D1, host computer) to a data store (D1, memory of unit 32).

Therefore, the subject-matter of **claim 13** is anticipated by the disclosure of D1, and thus **claim 13** does not meet the requirements of *Article 33(2) PCT*.

2.b Dependent method **claims 14 to 19**

Dependent **claims 14 to 19**, as far as they are dependent on **claim 13** for what concerns **claims 16 to 19**, do not add anything of inventive significance to **claim 13**. They either relate to standard practice of storing data or to standard communication means or well known types of data. Therefore, these claims do not meet the requirements of *Article 33(3) PCT*.

3.a Independent method **claims 8 and 12**

Claims 8 and 12 appear to relate to the transmission of electronic data from a data source to an apparatus and from an apparatus to a data store respectively.

There appears to be no real difference between the data source of **claim 8** and the apparatus of **claim 12** or between the apparatus of **claim 8** and the data storage of **claim 12**. Therefore, both claims are merely different from one another in that they use a different wording for defining the same subject-matter. Therefore, these claims lack of conciseness and thus do not meet the requirements of *Article 6 PCT*.

Having regard to **claim 8**, it is clear from point (v) that the encryption key has been set by the data source and copied by it to the apparatus during the previous communication. Therefore, it should be clearly defined in point (ii) that the determination of the encryption key is based on the apparatus identification code which is used to find that key. This is an essential feature because as the data source does not send back any information to the data receiving apparatus during the communication about the used encryption key, it is absolutely necessary that the data source uses the encryption key which the apparatus expects it has used. Otherwise the decryption in the data receiving apparatus will fail. The expression "thereby" is not considered to clearly enough define that the apparatus identity is used to retrieve the encryption key and therefore, also for this reason, **claim 8** does not meet the requirements of *Article 6 PCT*. The same observation applies to **claim 12**.

However, interpreting the expression in the sense as indicated above, it appears that the subject-matter of **claims 8 and 12** is new and involves an inventive step and thus these claims meet the requirements of *Article 33 PCT*.

3.b Dependent **claims 9 to 11 and 16 to 19**

Claims 9 to 11 and **claims 16 to 19,** as far as they are dependent on **claim 12**, also meet the requirements of *Article 33 PCT.*

Re. section VII

1. **Claim 13** appears to only include features which are also included in **claim 12**. Therefore, **claim 12** should be reworded as a dependent claim of **claim 13**, *Rule 6.3b PCT.*

INTERNATIONAL SEARCH REPORT

Inte nal Application No
PCT/GB 99/04219

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F12/14 G06F15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 08344 A (SACHS JAMES ;VIRTUAL PRESS (US); POMEROY THOMAS W (US)) 26 February 1998 (1998-02-26) abstract; figures 1,2A,2B page 5, line 1 -page 7, line 22 page 8, line 31 -page 8, line 36	1-12
A		13,14, 17-20
Y	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract; figure 3 page 4, line 2 -page 5, line 30 page 6, line 27 -page 10, line 6	1-12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 2000	24/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Sigolo, A

6

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 99/04219

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9808344 A	26-02-1998	US 5956034 A	21-09-1999
		AU 4148197 A	06-03-1998
		CN 1236450 A	24-11-1999
FR 2681165 A	12-03-1993	NONE	

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 23680	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/GB 99/ 04219	International filing date *(day/month/year)* 20/12/1999	(Earliest) Priority Date *(day/month/year)* 18/12/1998
Applicant JARMAN, David, Michael		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. _____

   [ ] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [X] None of the figures.

REPLACED BY ART 34 AMDT

friendly. Systems which have been proposed for use in this area include those described in EP-A-0665486, WO 95/08231 and WO99/12087, though the last of these does not form part of the state of the art. All seek to enhance the security against copying by using cryptographic techniques and generally require the use of encryption/decryption keys which are transmitted, after an authenticated request has been received, e.g. over a suitable communications link which has been established for that purpose.

The present invention provides apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data.

This approach, especially when used on a direct communications channel between user and information provider, rather than via a wide area network such as the internet, is advantageous as there is never any need to engage in a key request dialogue. Instead, an encryption/decryption key may be generated and used by reference to the addresses of resident code areas in ROM in the apparatus. This is explained in more detail below.

Claims

1 Apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data..

2 Apparatus according to claim 1 in which at least one encryption/decryption key is stored in a portion of either Electronically Erasable Programable Read Only Memory or non volatile Random Access Memory, and may be rewritten by an external key issuing computer.

3 Apparatus according to claim 2 in which at least one encryption key is 16 bytes in size.

4 Apparatus according to any one of claims 1 to 3 in which the Read Only Memory is at least 256 bytes in size.

5 Apparatus according to any one of claims 1 to 4 in which the data storage means is comprised of non volatile Random Access Memory.

6 Apparatus according to any one of claims 1 to 5 in which an output/input port is adapted to connect with a telephone socket via an electromagnetic radiation link.

7 Apparatus according to any one of claims 1 to 6 in which the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form.

8 Apparatus according to any one of claims 1 to 7 which is provided with a computer chip that has the specification, details and method of operation as set out on attached sheets marked A1, A2, A3, and A4.

9 A method of using apparatus according to any one of claims 1 to 8 for the reception of electronic data from an external data source characterised in that:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the user of the apparatus causes the apparatus to send a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that data and places it in the data

storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

10 A method according to claim 9 in which the means of electronic communication between the apparatus and the data source is via the telephone network.

11 A method according to claim 9 in which the means of electronic communication between the apparatus and the data source is via the internet.

12 A method according to anyone of claims 9 to 11 in which the electronic data is electronically stored text and/or graphics.

13 A method of using apparatus according to any one of claims 1 to 8 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the user of the apparatus causes the apparatus to transfer preselected data between the

apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

14 A method of using apparatus according to any one of claims 1 to 8 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store,

ii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

15 A method according to claim 14 in which the electronic data is transmitted from the data store to the apparatus, and is saved in the apparatus in decrypted form.

16 A method according to claim 14 in which the electronic data is transmitted from the apparatus to the data store, and is saved in the data store in encrypted form, the encryption key being a permanent encryption key for that data held in the apparatus.

17 A method according to any one of claims 13 to 16 in which the data store will on interrogation by the apparatus, provide the apparatus with a list of the data stored within the data store.

18 A method according to any one of claims 13 to 17 in which the means of electronic communication between the apparatus and the data store is via electrical or optical cable.

19 A method according to any one of claims 13 to 17 in which the means of electronic communication between the apparatus and the data store is via electromagnetic radiation.

20 A method according to anyone of claims 13 to 19 in which the electronic data is electronically stored text and/or graphics.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00, 12/14, 15/02 — A1

(11) International Publication Number: WO 00/38035

(43) International Publication Date: 29 June 2000 (29.06.00)

(21) International Application Number: PCT/GB99/04219

(22) International Filing Date: 20 December 1999 (20.12.99)

(30) Priority Data:
9828093.6 18 December 1998 (18.12.98) GB

(71)(72) Applicant and Inventor: JARMAN, David, Michael [GB/GB]; 11 Berkeley Street, Mayfair, London W1X 6BU (GB).

(74) Agent: GALLAFENT & CO; 9 Staple Inn, London WC1V 7QH (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: ELECTRONIC DATA STORAGE AND DISPLAY APPARATUS

(57) Abstract

Apparatus for displaying electronic format data is disclosed. It is particularly useful for displaying text material, e.g. as an electronic book. The apparatus has a casing with a display means such as a screen, and a data transmission/reception means enabling the apparatus to communicate with a source of data and to download data from the source for subsequent display. The data is encrypted for the download and decrypted within the apparatus to enable it to be displayed in clear. The distinctive feature of the invention is the use as an encryption/decryption key of data stored in addresses of a read only memory within the apparatus. Each time data is downloaded from the source, fresh addresses can be specified by the source, providing encryption/decryption keys for the next download session. This gives a very high degree of security as the keys themselves do not have to be transmitted.

PTO/PCT Rec'd 18 JUN 2001

Electronic data storage and display apparatus

This invention relates to electronic data storage and display apparatus, and in particular to such apparatus for the storage and display of electronic data that has commercial value such as electronically formatted books.

With the advances in the fields of microchip and display screen technologies, and allied computing advances it is becoming increasingly economically viable to produce apparatus that is easily portable and can store, manipulate and display large quantities of electronic data. There is, however, often a reluctance on the part of the owners of that data to release it to members of the public because of the ease of replication of electronic data. For data with commercial value such replication deprives the parties involved with the genesis and distribution of the data of a suitable reward for the production or distribution of that data. For example, if the data when rendered legible by suitable software is the text of a book, then if the data becomes available to the public not under the control of a distributor, copyright owner or the like, then if electronic copies of that data may easily be made, the publisher of that data and possibly others will suffer economic damage, for example being able only to sell fewer copies of a book than would otherwise be the case.

One approach is to render the data "copy-protected". This can be effective in some environments, though there is a widespread belief that copy-protection systems simply pose a challenge to those who would circumvent them. However, copy-protection systems which rely on encryption and decryption of data provide some effectiveness, for example as described in WO 97/44736. However, the system is cumbersome and not always user-

friendly. Systems which have been proposed for use in this area include those described in EP-A-0665486, WO 95/08231 and WO99/12087, though the last of these does not form part of the state of the art. All seek to enhance the security against copying by using cryptographic techniques and generally require the use of encryption/decryption keys which are transmitted, after an authenticated request has been received, e.g. over a suitable communications link which has been established for that purpose.

The present invention provides apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data.

This approach, especially when used on a direct communications channel between user and information provider, rather than via a wide area network such as the internet, is advantageous as there is never any need to engage in a key request dialogue. Instead, an encryption/decryption key may be generated and used by reference to the addresses of resident code areas in ROM in the apparatus. This is explained in more detail below.

In use, for example when the user of the apparatus wishes to obtain an electronic version of a book, the user connects the apparatus of the present invention to an appropriate source of electronic data in the following manner:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the user of the apparatus causes the apparatus to send a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that data and places it in the data storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

By having the apparatus and the data source interact in this fashion, the electronic data is encrypted when it is travelling between the owners or distributors of the data and the legitimate end user of the data. Because the encryption key between the data source and the apparatus is altered after each transaction, it will be very difficult for an illegitimate receiver of the data to decrypt that data. Even if that does prove possible,

the illegitimate receiver only then gains the encryption key for one specific piece of apparatus the next time it connects to the data source and not the data source as a whole.

In a particularly preferred embodiment of the present invention the apparatus stores two encryption keys, one of which is stored in either Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory, and the other of which is stored in Read Only Memory. The encryption key in the Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory is the key that is rewritten when the apparatus interacts with a data store.

In a preferred embodiment of the present invention, the encryption key in the Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory is 16 bytes in size. The portion of Read Only Memory, the content of which is used to encrypt/decrypt transmitted/received data, is preferably 256 bytes in size.

The data storage means in the apparatus of the present invention is preferably non-volatile random access memory. It may, however, alternatively be in the form of a magnetic disk, built into the casing and so constructed that attempts to remove the disc would result in the destruction of at least the data on the disc, or any other known data storage media which could be built into the casing.

The method of communication between the apparatus of the present invention and the data store is most preferably via the telephone network, and at least one input/output port in the casing is adapted to connect to that network most preferably via an electromagnetic radiation link.

In alternative embodiments other methods of connection the data source are possible and at least one input/output port in the casing is appropriately configured for that connection.

In a preferred embodiment of the present invention, the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form. The computer hardware preferably includes user control means which will allow a user of the apparatus to move through the data in an appropriate fashion. The display screen of the present invention is preferably of sufficient size that the viewing area thereof is at least 110mm by 180mm. The screen is preferably of a type that has a low power consumption.

In an alternative embodiment of the present invention, the apparatus additionally includes known means for the generation of sound. The sound generation means can be controlled by the computer software that controls the display means, or by independent control means. In this embodiment the reader of, for example, a book about ornithology may be played the sound of the bird which he is reading about.

It will be appreciated that the size of the data storage means in the apparatus of the present invention will be finite. As such, and to avoid the problem of either having to delete and loose a previously acquired set of data, or having to acquire a new apparatus, the apparatus of the present invention is configured so that it can export some or all of the data stored in the data storage means. To prevent duplicatable and readable copies of the data being exported, the apparatus is configured only to export the data in an encrypted form.

It is clearly desirable that the exported data can be imported back onto the apparatus of the present invention, so that the data can be viewed again at a later date.

The data is preferably exported to and imported from a dedicated data store adapted to interact with the apparatus of the present invention. In the first preferred embodiment, the method of transfer of the data is as follows:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

In a second preferred embodiment the method of transfer of the data is as follows:

i) the apparatus enters into electronic communication with the data store,

ii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

In this second embodiment the data store stores the data in encrypted form. Preferably there is, however, a little un-encrypted data attached to the encrypted data. That un-encrypted data can, for example, give an indication of the contents of the data, and/or the apparatus that placed the data in the data store and consequently the apparatus that can decrypt the data. This will allow more than one piece of apparatus of the present invention to use the data store.

In either of the two above described embodiments, the data transfer between the apparatus and the data store can be either via electrical or optical cables or via electromagnetic radiation.

The apparatus of the present invention may be provided with its own power source and/or means for taking power from an external power source.

In one particularly preferred embodiment of the present invention, the apparatus is provided with a computer chip that has the specification, details and method of operation as follows:

SPECIFICATION

EEPROM:	16 bytes of key memory (addresses 0 - 15). 112 bytes of user memory (addresses 16 - 127).
POWER:	5mA @5V when active 6mA @5V when writing to eeprom 10uA @5V in power saving mode.
CONVERSION RATE:	approx. 30KPS.

MASK LOOKUP TABLE

Rom address

0 = 255
1 = 254
2 = 253
3 = 252
4 = 251
5 = 250
.....
.....
.....
250 = 5
251 = 4
252 = 3
253 = 2
254 = 1
255 = 0

starting with address 0 = 255 the rom table is filled by the following formula :

rom table[address] = 255 - address

ENCRYPTION/DECRYPTION OPERATION

Version 1.0 of crypto uses a key length of 16 bytes.

First write the 16 byte key to eeprom addresses 0 - 15.
Each byte of key is used to access an 8 bit mask from within a 256 byte lookup table.
Each data byte is encrypted/decrypted by exclusive oring it with the 8 bit mask.
As each byte of data is encrypted/decrypted the mask is rotated one bit position to the left.
After eight bit rotations a new mask is loaded using the next key in the sequence of sixteen.
The sequence of masks will be repeated again when all sixteen have been used.

OPERATION MODES

EEPROM WRITE (mode 0)

1. Wait until BUSY line is a logic low.
2. Write number 0 (binary 00000000) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write eeprom address (0 - 127) to PORT1.
5. Wait until BUSY line is a logic low.
6. Write eeprom data to PORT2.

Steps 1 & 2 need only be done once to set eeprom write mode.

DECRYPT DATA (mode 1)

1. Wait until BUSY line is a logic low.
2. Write number 1 (binary 00000001) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write data for decryption to PORT2.
5. Wait until BUSY line is a logic low.
6. Read decrypted data from PORT3.

Steps 1 & 2 need only be done once to set data decrypt mode.

ENCRYPT DATA (mode 2)

1. Wait until BUSY line is a logic low.
2. Write number 2 (binary 00000010) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write data for encyption to PORT2.
5. Wait until BUSY line is a logic low.
6. Read encrypted data from PORT3.

Steps 1 & 2 need only be done once to set data encrypt mode.

EEPROM READ (mode 3)

1. Wait until BUSY line is a logic low.
2. Write number 3 (binary 00000011) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write eeprom address (0 - 127) to PORT2.
5. Wait until BUSY line is a logic low.
6. Read eeprom data from PORT3.

Steps 1 & 2 need only be done once to set eeprom read mode.

RESET COUNTERS (mode 4)

This will reset the rotate counter & key index to zero.

1. Wait until BUSY line is a logic low.
2. Write number 4 (binary 00000100) to PORT0.

POWER SAVING (mode 5)

This will put the crypto pcb into sleep mode.

1. Wait until BUSY line is a logic low.
2. Write number 5 (binary 00000101) to PORT0.
3. Wait until BUSY line is a logic zero before proceeding.

Waking up the crypto unit from power saving mode

1. Do a dummy read from PORT0 or Write a new operation mode to PORT0.
2. Wait until BUSY line is a logic low before proceeding.

20 WAY IDC CONNECTOR PIN OUT & DESCRIPTION

1.	GND	Power supply 0V connection.
2.	+5/3.3 VDC	Power supply positive connection.
3.	\RESET	Active low external chip reset. Leave disconnected if control of reset is not required. The chip takes approximately 80mS to reset after a low to high transition of the reset pin.
4.	\RD	Active low read control input.
5.	\WR	Active low write control input.
6.	\CS	Active low chip select input.
7.	A0	Port address select input.
8.	A1	Port address select input.
9.	D7	Bit 7 of bi-directional data bus.
10.	D6	Bit 6 of bi-directional data bus.
11.	D5	Bit 5 of bi-directional data bus.
12.	D4	Bit 4 of bi-directional data bus.
13.	D3	Bit 3 of bi-directional data bus.
14.	D2	Bit 2 of bi-directional data bus.
15.	D1	Bit 1 of bi-directional data bus.
16.	D0	Bit 0 of bi-directional data bus.
17.	BUSY	Active high busy output.
18.	\BUSY	Active low busy output.
19.	RxD	Serial data input (do not connect).
20.	TxD	Serial data output (do not connect).

Claims

1 Apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data..

2 Apparatus according to claim 1 in which at least one encryption/decryption key is stored in a portion of either Electronically Erasable Programable Read Only Memory or non volatile Random Access Memory, and may be rewritten by an external key issuing computer.

3 Apparatus according to claim 2 in which at least one encryption key is 16 bytes in size.

4 Apparatus according to any one of claims 1 to 3 in which the Read Only Memory is at least 256 bytes in size.

5 Apparatus according to any one of claims 1 to 4 in which the data storage means is comprised of non volatile Random Access Memory.

6 Apparatus according to any one of claims 1 to 5 in which an output/input port is adapted to connect with a telephone socket via an electromagnetic radiation link.

7 Apparatus according to any one of claims 1 to 6 in which the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form.

8 Apparatus according to any one of claims 1 to 7 which is provided with a computer chip that has the specification, details and method of operation as set out on attached sheets marked A1, A2, A3, and A4.

9 A method of using apparatus according to any one of claims 1 to 8 for the reception of electronic data from an external data source characterised in that:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the user of the apparatus causes the apparatus to send a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that data and places it in the data

storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

10 A method according to claim 9 in which the means of electronic communication between the apparatus and the data source is via the telephone network.

11 A method according to claim 9 in which the means of electronic communication between the apparatus and the data source is via the internet.

12 A method according to anyone of claims 9 to 11 in which the electronic data is electronically stored text and/or graphics.

13 A method of using apparatus according to any one of claims 1 to 8 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the user of the apparatus causes the apparatus to transfer preselected data between the

apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

14 A method of using apparatus according to any one of claims 1 to 8 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store,

ii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

15 A method according to claim 14 in which the electronic data is transmitted from the data store to the apparatus, and is saved in the apparatus in decrypted form.

16 A method according to claim 14 in which the electronic data is transmitted from the apparatus to the data store, and is saved in the data store in encrypted form, the encryption key being a permanent encryption key for that data held in the apparatus.

17 A method according to any one of claims 13 to 16 in which the data store will on interrogation by the apparatus, provide the apparatus with a list of the data stored within the data store.

18 A method according to any one of claims 13 to 17 in which the means of electronic communication between the apparatus and the data store is via electrical or optical cable.

19 A method according to any one of claims 13 to 17 in which the means of electronic communication between the apparatus and the data store is via electromagnetic radiation.

20 A method according to anyone of claims 13 to 19 in which the electronic data is electronically stored text and/or graphics.

INTERNATIONAL SEARCH REPORT

Intern. · onal Application No
PCT/GB 99/04219

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F12/14 G06F15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 08344 A (SACHS JAMES ;VIRTUAL PRESS (US); POMEROY THOMAS W (US)) 26 February 1998 (1998-02-26) abstract; figures 1,2A,2B page 5, line 1 -page 7, line 22 page 8, line 31 -page 8, line 36	1-12
A		13,14, 17-20
Y	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract; figure 3 page 4, line 2 -page 5, line 30 page 6, line 27 -page 10, line 6	1-12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 2000	24/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Sigolo, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. onal Application No
PCT/GB 99/04219

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9808344 A	26-02-1998	US 5956034 A	21-09-1999
		AU 4148197 A	06-03-1998
		CN 1236450 A	24-11-1999
FR 2681165 A	12-03-1993	NONE	

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
23680		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB99/04219	20/12/1999	18/12/1998
International Patent Classification (IPC) or national classification and IPC		
G06F1/00		
Applicant		
JARMAN, David, Michael		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
18/07/2000	20.03.2001
Name and mailing address of the international preliminary examining authority:	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx 523656 epmu d Fax +49 89 2399 - 4465	Van de Maele, L Telephone No. +49 89 2399 8805

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB99/04219

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:

Description, pages:

1,3-11	as originally filed			
2	as received on	04/01/2001	with letter of	29/12/2000

Claims, No.:

1-19	as received on	04/01/2001	with letter of	29/12/2000

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:
   - ☐ the claims, Nos.:
   - ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims 2-12,14-19
	No:	Claims 1,13
Inventive step (IS)	Yes:	Claims 8-12,16-19
	No:	Claims 1-7,13-15
Industrial applicability (IA)	Yes:	Claims 1-19
	No:	Claims

2. Citations and explanations
see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Cited documents:

D1: WO 98 08344 A
D2: FR 2 681 165 A

Re. sections V and VIII

1.a Apparatus **claim 1**

The subject-matter of **claim 1** does not appear to involve an inventive step having regard to the prior art disclosed D1.

D1 namely already describes, in correspondence with the preamble of **claim 1**, an apparatus for reception, storage and display of data in electronic format (D1, abstract and fig. 1, "14"). This apparatus also comprises data storage means, data display means and data transmission/reception means (D1, page 7, paragraph 3). Received data is decrypted and stored in the data storage means (D1, page 7, paragraph 3). It is not known from D1 to perform decryption in the reception means, however, D1 (page 7, third paragraph) teaches that this can be done by any combination of soft- and hardware and therefore selecting the reception means for this purpose is just one of the alternatives among which a skilled person would select. The apparatus of D1 also comprises storage means for storing an encryption key (D1, page 10, first paragraph).

According to the characterizing part of **claim 1**, the encryption key is only used to address the ROM to find the decryption key for the received data. Moreover, there are no features in **claim 1** which define a use of that key for encrypting. Therefore, this key is merely an index or pointer to the decryption key stored ROM of the apparatus. Document D2, which also describes an apparatus for receiving encrypted data, already teaches the use of an index into ROM (D2, page 4, lines 2 to 9) to retrieve the decryption key and to use the latter for decrypting the received data.

The apparatus defined in **claim 1** can not only receive encrypted data, decrypt it and store it in memory, it can also process the data in the reverse manner. It is

however explicitly indicated in D1 that this can also be done with the apparatus described therein (D1, page 6, first paragraph).

Therefore, all features of the claimed subject-matter of **claim 1** are known from D1 and D2. Both documents relate to the same problem of exchange of electronic information in encrypted form and thus the skilled person would consider combining the features known from these documents. Therefore, **claim 1** does not meet the requirements of *Article 33(3) PCT*.

1.b Dependent **claims 2 to 7**

The features of the dependent **claims 2, 5 and 7** are also already known from D1 (D1, pages 3. 7 and 10).

The features of **claims 3, 4** merely represent a choice of the key and memory size which does not appear to be relevant

Claim 6 merely defines the use of a well known type of communication link.

Therefore, none of the dependent claims appears to add an inventive step to the subject-matter of **claim 1** and thus also these claims do not meet the requirements of *Article 33(3) PCT*.

2.a Independent method **claim 13**

Claim 13 appears to merely define a method for transmitting encrypted data between two devices. Merely as an example, prior art document D1 already describes (D1, page 7, second paragraph) such a method for transmitting encrypted data from an apparatus (D1, host computer) to a data store (D1, memory of unit 32).

Therefore, the subject-matter of **claim 13** is anticipated by the disclosure of D1, and thus **claim 13** does not meet the requirements of *Article 33(2) PCT*.

2.b Dependent method **claims 14 to 19**

Dependent **claims 14 to 19**, as far as they are dependent on **claim 13** for what concerns **claims 16 to 19**, do not add anything of inventive significance to **claim 13**. They either relate to standard practice of storing data or to standard communication means or well known types of data. Therefore, these claims do not meet the requirements of *Article 33(3) PCT*.

3.a Independent method **claims 8 and 12**

Claims 8 and 12 appear to relate to the transmission of electronic data from a data source to an apparatus and from an apparatus to a data store respectively.

There appears to be no real difference between the data source of **claim 8** and the apparatus of **claim 12** or between the apparatus of **claim 8** and the data storage of **claim 12**. Therefore, both claims are merely different from one another in that they use a different wording for defining the same subject-matter. Therefore, these claims lack of conciseness and thus do not meet the requirements of *Article 6 PCT*.

Having regard to **claim 8**, it is clear from point (v) that the encryption key has been set by the data source and copied by it to the apparatus during the previous communication. Therefore, it should be clearly defined in point (ii) that the determination of the encryption key is based on the apparatus identification code which is used to find that key. This is an essential feature because as the data source does not send back any information to the data receiving apparatus during the communication about the used encryption key, it is absolutely necessary that the data source uses the encryption key which the apparatus expects it has used. Otherwise the decryption in the data receiving apparatus will fail. The expression "thereby" is not considered to clearly enough define that the apparatus identity is used to retrieve the encryption key and therefore, also for this reason, **claim 8** does not meet the requirements of *Article 6 PCT*. The same observation applies to **claim 12**.

However, interpreting the expression in the sense as indicated above, it appears that the subject-matter of **claims 8 and 12** is new and involves an inventive step and thus these claims meet the requirements of *Article 33 PCT*.

3.b Dependent **claims 9 to 11 and 16 to 19**

Claims 9 to 11 and **claims 16 to 19,** as far as they are dependent on **claim 12,** also meet the requirements of *Article 33 PCT.*

Re. section VII

1. **Claim 13** appears to only include features which are also included in **claim 12.** Therefore, **claim 12** should be reworded as a dependent claim of **claim 13,** *Rule 6.3b PCT.*

friendly. Systems which have been proposed for use in this area include those described in EP-A-0665486, WO 95/08231, WO 98/08344 and WO99/12087, though the last of these does not form part of the state of the art. All seek to enhance the security against copying by using cryptographic techniques and generally require the use of encryption/decryption keys which are transmitted, after an authenticated request has been received, e.g. over a suitable communications link which has been established for that purpose.

The present invention provides apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that the apparatus is configured such that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data.

This approach, especially when used on a direct communications channel between user and information provider, rather than via a wide area network such as the internet, is advantageous as there is never any need to engage in a key request dialogue. Instead, an encryption/decryption key may be generated and used by reference to the addresses of resident code areas in ROM in the apparatus. This is explained in more detail below.

Claims

1 Apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that the apparatus is configured such that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and so that the content of those addresses is used to encrypt/decrypt transmitted/received data.

2 Apparatus according to claim 1 in which at least one encryption/decryption key is stored in a portion of either Electronically Erasable Programable Read Only Memory or non volatile Random Access Memory, and may be rewritten by an external key issuing computer.

3 Apparatus according to claim 2 in which at least one encryption key is 16 bytes in size.

4 Apparatus according to any one of claims 1 to 3 in which the Read Only Memory is at least 256 bytes in size.

5 Apparatus according to any one of claims 1 to 4 in which the data storage means is comprised of non volatile Random Access Memory.

6 Apparatus according to any one of claims 1 to 5 in which an output/input port is adapted to connect with a telephone socket via an electromagnetic radiation link.

7 Apparatus according to any one of claims 1 to 6 in which the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form.

8 A method of using apparatus according to any one of claims 1 to 7 for the reception of electronic data from an external data source characterised in that:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the apparatus sends a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that data and places it in the data storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

9 A method according to claim 8 in which the means of electronic communication between the apparatus and the data source is via the telephone network.

10 A method according to claim 8 in which the means of electronic communication between the apparatus and the data source is via the internet.

11 A method according to any one of claims 8 to 10 in which the electronic data is electronically stored text and/or graphics.

12 A method of using apparatus according to any one of claims 1 to 7 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the apparatus causes the transfer of preselected data between the apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

13 A method of using apparatus according to any one of claims 1 to 7 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store,

ii) the apparatus causes the transfer of preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

14 A method according to claim 13 in which the electronic data is transmitted from the data store to the apparatus, and is saved in the apparatus in decrypted form.

15 A method according to claim 13 in which the electronic data is transmitted from the apparatus to the data store, and is saved in the data store in encrypted form, the encryption key being a permanent encryption key for that data held in the apparatus.

16 A method according to any one of claims 12 to 15 in which the data store will on interrogation by the apparatus, provide the apparatus with a list of the data stored within the data store.

17 A method according to any one of claims 12 to 16 in which the means of electronic communication between the apparatus and the data store is via electrical or optical cable.

18 A method according to any one of claims 12 to 16 in which the means of electronic communication between the apparatus and the data store is via electromagnetic radiation.

19 A method according to anyone of claims 12 to 18 in which the electronic data is electronically stored text and/or graphics.